100. (previously presented) The method of claim 99 which includes as a preliminary step authenticating a signer as authorized to sign.

101. (previously presented) The method of claim 99 whereby the server uses a symmetric key to digitally sign.

102. (previously presented) The method of claim 99 whereby the server uses a MAC to digitally sign.

103. (previously presented) The method of claim 99 whereby the server uses XMLDSIG to digitally sign.

104. (previously presented) The method of claim 99 whereby the GUID is used as a password or seed for a symmetric cipher that is used to encrypt a message digest as a digital signature.

105. (previously presented) The method of claim 99 whereby the GUID is used as a password or seed for a symmetric cipher that is used to encrypt an asymmetric signature value as a digital signature.

106. (previously presented) The method of claim 99 whereby the GUID is used as a password or seed for a symmetric cipher that is used to encrypt the text, binary object, or combination of form input and a document template to be signed as a digital signature.

107. (previously presented) The method of claim 99 whereby the digital signature is a detached digital signature.

108. (previously presented) The method of claim 99 whereby a detached digital signature is stored in a data store as a part of a signature transaction record.

109. (previously presented) The method of claim 99 whereby a message digest is stored in a data store as a part of a signature transaction record.

110. (previously presented) The method of claim 99 whereby a symmetrically encrypted message digest is stored in a data store as a part of a signature transaction record.

111. (previously presented) The method of claim 99 whereby a symmetrically encrypted detached digital signature value is stored in a data store as a part of a signature transaction record.

112. (previously presented) The method of claim 99 whereby the server sends a notification to a signer or her designee of the occurrence of a signature transaction.

113. (previously presented) The method of claim 99 whereby a human being is a signer on whose behalf a signature is affixed.

114. (previously presented) The method of claim 99 whereby a computerized agent is a signer on whose behalf a signature is affixed.

115. (previously presented) The method of claim 99 whereby a business or governmental entity is a signer on whose behalf a signature is affixed.

116. (previously presented, currently amended) ~~A method~~ An apparatus to electronically sign text and objects (defined as files, documents, or transaction data) for and on behalf of another comprising:

a. a website for signing that includes
   i. a clock for determining date and time values,
   ii. at least one web page to present and display to a user for inputting information and submitting it to ~~said~~ a server computer;
   iii. an encryption key
   iv. a hashing algorithm,

v. an optional file or data store with at least one template with prepared text; and

vi. a data store for the storage of a plurality of records of signature transaction data;

b. a signer with a computer or handheld computing device having a display to view information provided by such web server and a keyboard, keypad, touchscreen, touchpad, or stylus to input text and a pointing device;

c. a network connection between the computers;

d. said ~~method~~ apparatus further ~~consisting of~~ performing the following steps:

i. said website providing an electronic form to a signer, said form having a plurality of inputs to:

1. identify a signer;
2. identify a credit card ~~to charge for the service~~ for payment;
3. provide character input for text, and/or to upload at least one object to be signed;
4. supply a password or personal identification number where authentication of identity by means of a password or personal identification number is required; and
5. submit the other inputs to said server;

ii. where authentication of a signer's identity is required before signature, a processing unit of said website comparing an inputted password, personal identification number, digital certificate, biometric identifier, or combination thereof, with a stored record before taking any further action on the basis of such authentication;

iii. where authentication of a signer's identity is established or is not required,

1. where text has been inputted by a signer for combination with a transaction template at a server of said website for signature, combining said text with a transaction template and displaying the combination to the signer as input to be signed;
2. by means of said message digesting algorithm, calculating a message digest of each input to be signed;

3. by means of said encryption key, generating an encrypted value of each said message digest;
4. displaying a warning that activation of a displayed input to sign will operate as a binding signature of the signer and offering a displayed alternative input to cancel a further signature operation;
5. upon activation of said displayed input to sign, said server creating a signature transaction record and storing the same in a data store of signature transaction records.
6. transmitting a receipt and proof of signature containing the unique signed data and signature value to the signer.

117. (previously presented, currently amended) The ~~method~~ apparatus of claim 116 wherein an encrypted message digest is a detached digital signature.

118. (previously presented, currently amended) The ~~method~~ apparatus of claim 116 wherein the detached digital signature is encrypted by means of a symmetric key.

119. (previously presented, currently amended) The ~~method~~ apparatus of claim 116, wherein data that associates the identity of an authorized signer with the entity's digital signature is a signature transaction record consisting of a message digest and encrypted message digest of the data, and optionally, one or a plurality of the following;

a. a date of signature,
b. a time of signature,
c. a generated nonce,
d. a credit card authorization,
e. a network address from whence a request to sign originated,
f. the signer's name identifier;
g. a unique identifier assigned to the signature transaction record;
h. an email address of the signer;
i. one or a plurality of properties of a digital certificate issued to the signer;
j. a representation of one or a plurality of biometric identifiers of the signer.

120. (previously presented, currently amended) The ~~method~~ apparatus of claim 118 wherein the symmetric key is derived from a password or seed of composed of one or a plurality of values, or message digest thereof, contained in the signature transaction record.

121. (previously presented, currently amended) The ~~method~~ apparatus of claim 116 whereby a confirmation of a signature transaction is transmitted to a signer from a remote signing computer as proof of an authentic signature transaction.

122. (previously presented, currently amended) The ~~method~~ apparatus of claim 121 whereby upon receipt, the proof of an authentic signature transaction is subsequently signed by a recipient using a private asymmetric key associated with a digital certificate of the recipient as an act of signature.

123. (previously presented, currently amended) The ~~method~~ apparatus of claim 116 wherein the message digest is encrypted by means of a symmetric key.

124. (previously presented, currently amended) The ~~method~~ apparatus of claim 123 wherein the symmetric key is derived from a password or seed of one or a plurality of values, or message digest thereof, contained in the signature transaction record.

125. (previously presented, currently amended)The ~~method~~ apparatus of claim 116 wherein the data submitted for signature consists of one or a plurality of the following:

a. data that is supplied by a user to a remote computer through submission of one or a plurality of inputs to one or a plurality of forms,
b. data that is supplied by a user to a remote computer through submission of one or a plurality of inputs to one or a plurality of forms, in combination with a template supplied by a remote computer,

c. a file,
d. a message,
e. a document,
f. a message digest,
g. transaction data,
h. XML data,
i. programming code,
j. a document containing mark-up,
k. one or a plurality of units of currency,
l. a legal document,
m. a medical record,
n. a prescription,
o. a promise,
p. a promissory note,
q. a contract,
r. a mortgage or deed of trust,
s. a purchase order,
t. text,
u. one or a plurality of numbers,
v. a conveyance,
w. a transaction record,
x. one or a plurality of dates,
y. a check or money order,
z. binary data.

126. (previously presented, currently amended) The ~~method~~ apparatus of claim 116 whereby upon a successful signature verification, the remote computer sends a message as proof of a verified signature transaction.

127. (new, previously cancelled) A method for signing and verifying electronic data by or on behalf of another at server comprising:

a. an authentication step of creating a collection of records about a plurality of individuals by entering into a data storage medium a collection of any or a combination of any of the following:
   i. personal information about an individual,
   ii. an indicator of the reliability of the identification of the individual who is the subject of a record,
   iii. whether the authentication mode is universal or whether such individual must authenticate to the server computer in order to sign electronic data using the server computer, and
   iv. the authentication credential or plurality of authentication credentials that such individual must present to the server in order to sign;

b. an access control step of
   i. receiving a request to sign and, unless the authentication mode is universal, an authentication credential or a plurality of authentication credentials from a requestor, and
   ii. comparing the authentication credential or credentials to the information contained in the collection of records to determine if the requestor is an individual who is authorized to sign electronic data using the server;

c. a presentation step of providing to the server an electronic data set for signature;

d. a transaction identifier step of generating at the server a globally unique transaction identifier for the electronic data that a requestor intends to sign, which includes as one input an identifier associated with the requestor's identity;

e. a signature step whereby the server encrypts, as the signature of a signer, each electronic data set with a unique encryption key, generated from a symmetric cipher using the globally unique transaction identifier as the character input of a password for generation of the key;

f. a recording step in which the server generates and stores in a data storage medium a record of a signature transaction;

g. a verification step whereby

i. an inquiring party seeking to verify the validity of a signature of electronic data transmits to a server electronic data that is believed to have been previously signed at a server;

ii. the server determines if a record or a plurality of records corresponding to the transmitted electronic data exists in the data storage medium of such records;

iii. the server retrieves a record or plurality of records corresponding to the electronic data which is presented for verification;

iv. with regard to each such record, the server performs a verification operation which includes a step of reconstructing a symmetric cipher from a record of input for a password of a key that was used to create an encryption key initially, including an identifier of the signer, and applying such symmetric cipher to decrypt an electronic data set;

v. After decryption, the server reports to an inquiring party,

1. whether an electronic data submitted for verification remains unmodified since a signature was affixed, and

2. the identity of a signer of the electronic data.

128. (new, previously cancelled) The method of claim 127 wherein the electronic data set which is symmetrically encrypted during signature and decrypted upon verification at a server consists of one of the following:

a. A message digest or hash of the electronic data;
b. A crypto-transformation, created using a private key, of the message digest or hash of the electronic data.

129. (new, previously cancelled) The method of claim 76 wherein the electronic data submitted for signature consists of one of the following:
a. Form input of a signer;
b. A combination of form input of a signer and standardized words, clauses, or phrases.